n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ where k is an integer greater than 2, p_1, p_2, ... p_k are distinct prime numbers, and where C is a number representative of an encoded form of message word M, wherein said encoding step comprises the step of:

transforming said message word signal M to said ciphertext word signal C whereby

$$C_1 = M_1^{e_1} \bmod p_1$$
$$C_2 = M_2^{e_2} \bmod p_2$$
$$\vdots$$
$$C_n = M_n^{e_n} \bmod p_n,$$

$$M_1 = M \pmod{p_1},$$
$$M_2 = M \pmod{p_2},$$
$$\vdots$$
$$M_n = M \pmod{p_n},$$
$$e_1 = e \bmod (p_1-1),$$
$$e_2 = e \bmod (p_2-1),$$
$$\vdots$$
$$e_n = e \bmod (p_n-1)$$

where e is a number relatively prime to $(p_1-1) \cdot (p_2-1) \cdot \ldots \cdot (p_k-1)$,

$$Y_i = Y_{i-1} + \left[(M_i - Y_{i-1}) (w_i^{-1} \bmod p_i) \bmod p_i \right] \cdot w_i \bmod n$$

for $i \geq 2$ and

$$C = Y_k,\ Y_1 = M_1,\ and\ w_i = \prod_{j<i} p_j\ .$$

15. The method according to claim 1, comprising the further step of:

decoding the ciphertext word signal C to the message word signal M, wherein said decoding step comprises the step of: transforming said ciphertext word signal C, whereby:

$$Y_i = Y_{i-1} + \left[(M_i - Y_{i-1})\,(w_i^{-1} \bmod p_i) \bmod p_i \right] \cdot w_i \bmod n$$

where $i \geq 1$ and

$$M = Y_k,\ Y_1 = C_1,\ and\ w_i = \prod_{j<i} p_j\ .$$

16. A cryptographic communications system comprising:

a communication medium;

an encoding means coupled to said communication medium and adapted for transforming a transmit message word signal M to a ciphertext word signal C and for transmitting C on said channel, where M corresponds to a number representative of a message and

$0 \leq M \leq n-1$ where n is a composite number of the form

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

where k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct prime numbers, and where C corresponds to a number representative of an enciphered form of said message and corresponds to

$$C \equiv M^e \pmod{n}$$

where e is a number relatively prime to $\mathrm{lcm}(p_1-1, p_2-1, \ldots, p_k-1)$; and

a decoding means coupled to said communication medium and adapted for receiving C from said channel and for transforming C to a receive message word signal M′ where M′ corresponds to a number representative of a deciphered form of C and corresponds to

$$Y_i = Y_{i-1} + \left[(M_i / - Y_{i-1}) \, (w_i^{-1} \bmod p_i) \bmod p_i \right] \cdot w_i \bmod n$$

where $i \geq 1$ and

$$M = Y_k, \; Y_1 = C_1, \; and \; w_i = \prod_{j<i} p_j \, .$$